Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Security-First Data Engineering: Best Practices for Compliance in Healthcare and Financial Data Pipelines

Sushil Kumar Tiwari
Independent Researcher, USA

ARTICLE INFO

Received: 05 Sept 2025

Revised: 15 Oct 2025

Accepted: 25 Oct 2025

ABSTRACT

Security-First Data Engineering Framework (SF-DEF) is a holistic approach to intrinsically integrate security, privacy, and compliance in data pipeline solutions in both healthcare and financial industries. With a transition to proactive integration across the data lifecycle, replacing the classical frameworks of reactive security with the enabling of major vulnerabilities in the transformation processes, SF-DEF can meet complex regulatory standards such as HIPAA, GDPR, PCI-DSS, and SOX. The framework has seven fundamental security principles, namely data minimization, zero trust architecture, encryption by default, role-based access controls, automated compliance validation, immutable logging and data masking, which provide defense-in-depth protection and simplify compliance management. Experimental assessments in both health and financial settings reveal extensive enhancements in policy violation identification, security efficacy, and audit efficacy under constant review and automated checking, which converts the compliance to an intermittent operational trait.

Keywords: Data Security, Compliance Automation, Zero Trust Architecture, Healthcare Data Protection, Financial Data Pipelines

I. Introduction

Information has become a strategic asset to innovation in both the healthcare and financial industries, serving as the catalyst for techniques of high-level diagnostics and high-technology financial analytics. Instead, the medical facilities now use huge collections of patient data to improve treatment outcomes, whereas financial entities use transaction-related data to assess risks and stop fraud cases. This development is a paradigm shift in the functioning of the regulated industries in the digital environment and opens new possibilities for efficiency in their operations and performance [1].

Nonetheless, this data transformation introduces more security risks and compliance issues. Enterprises are exposed to advanced Internet threats that concern data streams directly, and consumer privacy issues are expanding. These issues pose serious operational demands as institutions balance the innovation needs on one hand, and the need to enhance security in more complex technical environments on the other [2].

Traditional data engineering methods had traditionally viewed security as a post-hoc data-related consideration, meaning they put in place controls once architectural decisions were made. This dynamic paradigm poses inherent weaknesses in that security thinking is not incorporated at the early stages of design. When protective controls and measures are not combined with core architecture but are appended to existing systems, organizations often find security problems at integration points, and the protective controls and functional requirements clash. These constraints are particularly disastrous within controlled settings where legal systems require overarching security across the data lifecycle [1].

The regulatory environment is becoming more and more complex and stringent. Medical institutions have to navigate the HIPAA standards that provide extensive security for the safeguarded health data. Payment data Covers: Financial institutions have the systems of the PCI-DSS, which address customer information within Europe under the GDPR, and SOX, which addresses financial reporting integrity. These overlapping regulations not only provide concrete technical controls but also provide governance expectations and audit requirements, resulting in enormous overhead operations and compliance risk [2].

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

There is a considerable gap in the methodology of incorporating security in the data engineering processes. Whereas the studies focus on security controls and compliance frameworks in isolation, less research has focused on how the two factors can be directly represented in the pipeline structure. The disconnection between data engineering and security disciplines frequently creates disjointed implementations that fail to reflect the natural connections between data flows and security requirements and the resultant complexity and potential vulnerabilities [1].

Security-First Data Engineering Framework (SF-DEF) solves these issues by making security, privacy, and compliance design principles instead of peripheral considerations. This model appreciates the fact that the protection of data should start at the architecture design and proceed to implementation and operation. Through integrating security at every phase of the engineering process, organizations can develop resilient systems that can satisfy compliance standards and support business goals. The framework incorporates pre-existing security standards such as data minimization, zero trust architecture, encryption as default, access controls, compliance checking and validation, extensive audit logs, and privacy-preserving methods directly into the design of a data pipeline [2].

II. Literature Review

The historical development of traditional data engineering solutions has gone through various stages, starting with primitive batch-based solutions to the current streaming solutions. An early use of these applications tended to focus more on security by maintaining perimeter defenses, based on network segregation and database-level protections instead of pipeline-specific protections. The idea of this architecture was based on the historical computing paradigms in which physical infrastructure boundaries were used to provide natural security demarcation. With the shift of data engineering to distributed systems, security implementations continued to be mostly endpoint-oriented instead of being implemented across processing workflows. The prevailing security model focused on securing the data stores but offered little protection to the data in the transition phases, which posed major vulnerabilities in the processing phases [3].

Healthcare and financial data regulatory systems have developed a complicated compliance environment that organizations have to operate within. Healthcare facilities should adopt the HIPAA requirements that entail the provision of overall protective measures on protected health information, including specific administrative, physical, and technical controls. The burden of regulation levels rises significantly because of organizations in charge of financial information, where PCI-DSS defines specific standards of payment card environments, GDPR sets extensive data protection of European subjects, and SOX forms strict controls regarding financial reporting devices. Every framework presents its own unique demands, testing procedures, and implementation tools that pose significant levels of compliance complexities for organizations in a variety of regulated areas [3].

Zero Trust Architecture is a groundbreaking change in the thinking of security that has been transformed from theory to implementation frameworks during the last ten years. The basic premise in this technique is that implicit trust, in this case, is rejected in favor of constant validation of all interactions of the system, irrespective of source. Applied to data engineering, ZTA principles mandate that authentication and authorization be performed at every stage of the pipeline, erasing traditional trust boundaries among pipeline components. This method has solved the vulnerabilities that are critical in the traditional models, especially in the transformation stages where sensitive data are subjected to processing. Although the implementation issues are still considered to be a significant number, particularly in legacy markets with well-established trust relationships, the security advantages are enhanced breach containment and low lateral movement capabilities of potential attackers [4].

III. Security-First Design Principles

Minimization of data sets can create basic security prevention by minimizing the possible data-exposure platforms by cautiously limiting data gathering and storage. This principle is a philosophical change of the traditional methodology of extensive collection of data to a specific acquisition that would meet specific and documented needs of the business. The process starts at the lowest levels of pipeline design with a detailed schema planning, which ensures that all superfluous fields are removed and that the purpose of each data element is specified. The techniques involve schema enforcement methods that reject unnecessary attributes, automatic classification of sensitive elements that are to be treated specially, and

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

dynamic field-level filtering by looking at the processing situation. In addition to the original limitations of collection, extensive implementations create lifecycle management involving automated retention enforcement, purpose expiration, and secure deletion procedures [3].

Zero Trust Architecture implemented on data pipelines needs to take a fundamental re-evaluation of the interaction between pipeline elements and authentication. Instead of building trust on network boundaries, every component of the pipeline, such as extraction services, transformation functions, orchestration tools, and storage systems, has to authenticate on its own and run with as few privileges as possible. The process normally starts with identity infrastructure modernization, which provides robust authentication mechanisms of human identity as well as service identity across the pipeline ecosystem. Service-to-service communications must be mutually authenticated, and this authentication is not dependent on the network location, and is usually implemented using mutual TLS (mTLS) authenticators that authenticate both the client and server identity of each connection. Contextual risk assessment is part of access decision-making, and it is based on aspects such as the origin of the request, past behavioral patterns, sensitivity of the data, and the current risk intelligence [4].

Principle	Key Components	Implementation Approach
Data Minimization	Purpose specification, Schema enforcement	Field elimination, Automated classification
Zero Trust Architecture	Component authentication, Minimal privileges	mTLS implementation, Contextual evaluation
Encryption by Default	Multiple protection layers, Key management	Transport encryption, Storage protection
Role-Based Access Control	Job function alignment, Contextual factors	Identity infrastructure, Attribute extensions
Automated Compliance	Continuous validation, Evidence collection	Policy-as-code frameworks, Runtime monitoring
Immutable Logging	Tamper-resistant records, Forensic support	Cryptographic verification, Detailed activity recording
Data Masking	Protected identifiers, Analytical utility	Format preservation, Tokenization techniques

Table 1: Security-First Design Principles [3, 4]

The default encryption makes the strategies of protection selective and applied only to the most sensitive parts within holistic protection mechanisms throughout the data lifecycle. This principle focuses on the protection of the data in all its states: in rest, transit, processing, etc., as opposed to the vulnerability points. Technical implementation is an action that needs to enable coordination among several layers of protection, which starts with transport encryption that ensures important data transfer over TLS 1.3 or other equivalent protocols. Storage protection usually uses transparent encryption on a volume and object level, and application-level encryption presents extra protection to especially sensitive elements. Key management is one of the most important implementation factors, which demands separation between the operation of encryption and key management, periodically planned key management rotation processes, and secure storage using hardware security modules or dedicated key management services [3].

IV. Methodology

The Security-First Data Engineering Framework (SF-DEF) architecture is a system that provides a systematic method of incorporating security into the data processing processes. The framework assigns security implementation in functional layers that meet different aspects of the data lifecycle, but which work as a system. Each of the layers has certain controls related to vulnerabilities that are likely to be exploited during the corresponding processing stage, and security mechanisms are designed to interact and achieve defense-in-depth protection. The architecture focuses on modularity, which enables organizations to deploy the architecture components in stages as per their risk ranking instead of having to deploy the entire architecture before achieving returns. This is a method that appreciates the pragmatic

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

facts of change management in an organization, where small-step implementation can be more productive than a wholesale change endeavor [5].

The integration methodology deals with both technical and organizational aspects of the security implementation, considering that technology would not be enough without the relevant process modifications and inter-functional cooperation. Technical integration embraces infrastructure-as-code models that specify security controls and functional elements, which ensure that deployment is consistent across environments and removes security lapses, which otherwise would arise due to manual implementation. Organizational integration aims at creating collective responsibility patterns among data engineering, security, and compliance groups, where each has a well-defined role during the development lifecycle. The implementation process is usually done in phases, starting with the current state assessment and then a reference architecture development, pilot implementation including high-value use cases, and finally a broader implementation with continuous improvement mechanisms [6].

The experimental assessment used synthetic data that simulated healthcare and financial settings, specifically, constructed to have real-life complexity, but without privacy and regulatory issues related to actual production data. Statistical modeling of production pattern based synthetic generation process was used, with guaranteed realistic data distribution, relationship, and edge case, as well as full control on sensitive elements placement. This technique allowed thorough testing of security in a variety of data types, forms as well and processing conditions without exposing real secured information. Test environments were of various types of infrastructure, e.g., cloud platform and on-premises systems, which reflects the reality of enterprise data ecosystems being heterogeneous. The experimental design involved both functional testing, which was used to determine the effectiveness of security mechanisms, and performance testing, which was used to determine overhead effects under realistic operational loads [5].

V. SF-DEF Detailed Architecture

The Secure Ingestion Layer creates controlled portals to all incoming data into pipeline environments, which is a vital first security point, where any external data is first placed under the control of the organization. The layer deploys a defense-in-depth option, which integrates various security interventions in averting bad data entry, authenticity of the source, and adherence to structural mandates prior to being introduced into the processing processes. Implementations of API gateways provide uniform authentication, authorization, and validation of all sources and formats, and remove security inconsistencies of ingestion mechanisms typically found in environments with multiple ingestion mechanisms. These gateways also apply common security patterns such as token validation, rate limiting, schema enforcement, and anomaly detection to reject potentially malicious inputs before they are passed to processing stages [5].

The Transformation and Encryption Layer helps in overcoming security difficulties at the stages of data manipulation, which is the least protected pipeline stage in general, as processing requirements tend to be incompatible with protection mechanisms. The containerized transformation environments are isolation environments that give each processing function an independent execution environment and avoid lateral movement between components, as well as restricting possible blast radius in the event of a security incident. This architectural method is a substantial difference from the past transformation implementation, where there are usually several functions working within similar environments, with low security boundaries. The implementation makes use of container orchestration platforms to support security settings such as mandatory access controls, network policies that apply micro-segmentation, and resource constraints that avoid denial-of-service states [5].

Layer	Primary Function	Key Security Mechanisms
Secure Ingestion	Entry point control	API gateways, Schema validation, Anomaly detection
Transformation & Encryption	Processing security	Containerization, Isolated execution, Field-level protection
Compliance Control	Regulatory alignment	Preventive controls, Detective mechanisms, Automated remediation
Access & Identity	Authorization	Centralized IAM, Federation support, Context-

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Management	framework	based decisions
Monitoring & SIEM	Threat detection	Real-time alerting, Correlation analysis, Behavioral monitoring
Governance & Audit	Documentation & verification	Metadata logging, Lineage tracking, Evidence collection

Table 2: SF-DEF Architecture Layers [5, 6]

The Compliance Control Layer creates continuous verification of compliance with the regulatory requirements, and compliance ceases to be a result of periodic evaluation; it becomes an ongoing operational attribute. This architecture is a detect-prevent-remediate model that focuses on compliance across the pipeline lifecycle. Preventive controls are combined with development processes to prevent deploying non-compliant configurations, and detective controls are used to continuously check runtime environments that show a drift in compliance that needs to be addressed. Workflows of remediation automatically deal with frequent compliance problems in which automated resolution is possible, and complex situations are left to human intervention where required. This architectural design fundamentally transforms the compliance management approach away a reactive style to a proactive approach that discovers potential problems before they affect the compliance status, as opposed to finding out the problems in the audit processes where remediation causes operational disruption [6].

VI. Results and Analysis

A clinical assessment of the SF-DEF implementation showed significant gains in the most important security and compliance measures in case of applying it to healthcare and financial data pipelines. The mechanisms used to discover policy violations detected potential compliance problems much higher than usual periodic audit methods, and allow remediation of the problem before organizational compliance status could be affected. This proactive identification was found specifically useful to deal with problems during the stage of transformation, where the data may more often than not pass through several manipulation steps, and this can, as a result, release the sensitive information unintentionally. The entire monitoring of all the pipeline phases of the framework enhanced transparency in the closed areas of processing, exposing non-compliance issues that, until security breaches or external audits, had remained unknown [7].

The effectiveness assessment of security has demonstrated notable success in prevention and containment that is far superior to the traditional methods. The use of access control mechanisms proved to be more protective against unauthorized access attempts, and persistent authentication and contextual authorization helped to avoid misuse of credentials in the traditional models. The implementation of zero-trust was especially useful against the attempts of lateral movement, as attackers could not use the initial access to reach the adjacent system with sensitive information. These advances are based on the underlying architectural modifications of the framework and not the incremental upgrades, but they are built-in security modifications that are not added as peripheral restrictions to the design of pipelines. The holistic method eradicated component security holes that had been the points of vulnerability of the components during an advanced attack [8].

Domain	Security Improvements	Compliance Advantages	Operational Enhancements
Healthcare	PHI protection throughout the lifecycle	HIPAA technical safeguard alignment	Streamlined audit preparation
Financial Services	Transaction security	Multi-framework control unification	Reduced compliance overhead
Cross-Domain	Breach prevention capabilities	Unified control implementation	Automated evidence collection
Data Engineering	Transformation stage protection	Continuous validation	Pipeline visibility

Table 3: Implementation Benefits by Domain [7, 8]

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The case study of the healthcare implementation system revealed the effectiveness of the framework in ensuring the safety of sensitive information related to patients during work processes. Implementation provided the overall controls that covered the HIPAA technical safeguard requirements by the combination of access control, extensive activity logs, integrity checks, and transmission protection. PHI was made visible depending on specific job functions, and attribute-based extensions were used to limit access depending on contextual aspects such as location, device characteristics, and access patterns. Extensive audit documentation provided detailed documentation of all PHI interactions, which can be used to monitor security as well as verify compliance. PHI identification was automated, which protected unstructured PHI, such as clinical notes and transcriptions, overcoming a frequent vulnerability of prior systems that often poorly secured sensitive data in text fields [8].

VII. Discussion

Implementation results analysis showed that the patterns of implementation were similar in different organizational settings, and some of the most critical factors that contribute to improved results are than that are not achieved through traditional methods. The transition of reactive to proactive security implementation is a paradigm shift in how organizations look at the issue of data protection because they think of protection controls at the earliest stages of the design, and do not add the protection measures after the architectural decisions have been made. This model removes numerous compromise cases encountered with the conventional methods of implementing such solutions, where retrofitted security controls are likely to be incompatible with existing architectural patterns. The subsequent correspondence between security systems and business needs lessens friction across development lifecycles and, at the same time, enhances the effectiveness of protection by more fully integrating with processing workflows [7].

The benefits of compliance management are not only in the realization of a better level of control but also in significant operational benefits that are enjoyed in the course of regulatory procedures. Continuous validation strategy converts compliance into a periodical disruptive evaluation into the continuous operational feature without the resource-consuming remediation cycles that occur in conventional set-up, where the problems are not discovered until during audit periods. Such a strategy provides certain benefits to companies whose work is in a highly dynamic regulatory environment in which the instability of requirements is adapted much faster than periodic assessment models. The automated evidence gathering systems also promote compliance operations by creating the necessary documentation in the course of regular processing as opposed to specific collection action and lower the burden of preparation as well as the possible lapses in documentation when evaluations are being conducted [7].

Unified control implementation is a regulatory alignment that is used to counter a crucial problem that organizations that work within multiple compliance systems know, but that are characterized by inconsistently designed requirements. The conventional methods often have distinct controls for each regulatory framework, which have duplication, possible inconsistency, and unnecessary maintenance needs. The control mapping approach to the framework allows the efforts of a single implementation to fulfill the needs of more than one regulation at once, limiting the complexity of implementation and the maintenance load on the systems to be borne dramatically. This method is especially helpful in the challenging regulatory context, such as healthcare financial operations, which need to meet the needs of healthcare privacy, financial reporting, and payment security frameworks with the help of unified control implementation [8].

VIII. Future Research Directions

Federated learning is an excellent field of study in the privacy-preserving analytics of controlled settings that allow organizations to learn using distributed datasets, ensuring data locality and regulatory adherence. The model should be seen as fundamentally changing the nature of analytical methods as it places computation on data instead of concentrating on sensitive data, which is a fundamental privacy issue in conventional analytics. Federated methods are especially useful in medical and financial practice, where privacy laws often pose a hindrance to conventional consolidated analysis. Federated learning enables cross-organizational collaboration opportunities with a chance of cross-organizational data sharing because of maintaining data boundaries at an organizational level and only sharing model updates instead of sharing actual data. Initial prototypes show that it can offer advanced analytical tasks

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

such as predictive modelling, anomaly detection, and pattern recognition, and have high privacy guarantees [9].

Compliance tracking built on blockchain provides new solutions to the creation of audit trails that are verifiable and record compliance with the regulations at the data lifecycle stages. It is a methodology that uses distributed ledger technology to come up with immutable records of compliance activities, security controls, and data handling practices appropriate to undergo regulatory checks. The base level of resistant tampering of blockchain structures helps to overcome inevitable shortcomings of traditional audit strategies, where records of compliance may be distorted themselves as part of advanced assaults. Such a method comes in handy, especially when showing consistent compliance as opposed to point-in-time, establishing chronological records of the implementation of control during the processing activities. Regulated industries show a specific potential in regards to a privately implemented blockchain, where the security benefits of distributed verification can be attained without compromising the confidentiality that sensitive compliance data may require [9].

AI-controlled adaptive security is a new research field that aims to improve threat detection and response with predictive analytics and automated orchestration. This is a machine learning that uses piping telemetry to detect behavioral patterns that may indicate vulnerability to security threats before exploitation. In contrast to conventional rule-based systems, which use known signatures, adaptive techniques may be useful in detecting new attack patterns by detecting behavioral deviation based on behavior change in response to the increasingly sophisticated threats to data pipelines. Supervised learning methods that were trained on labeled security events have shown potential in the detection of known threats, and unsupervised and semi-supervised methods have the potential to detect previously unknown attack patterns through behavioral anomalies. In addition to detection, reinforcement-based learning algorithms demonstrate potential in automated coordination of responses, possibly choosing the right mitigation actions without human intervention that relies on the observed characteristics of the attack and the situation of the system [10].

Direction	Core Concept	Potential Applications
Federated Learning	Privacy-preserving analytics	Cross-organizational collaboration without data sharing
Blockchain Compliance	Immutable audit trails	Cryptographic verification of regulatory controls
AI-Driven Security	Predictive threat detection	Automated response orchestration
Carbon-Aware Security	Environmental sustainability	Energy-efficient cryptographic algorithms

Table 4: Future Research Directions [9, 10]

Carbon-conscious security optimization is a new research agenda that deals with the possible conflicts between the full security application and the objective of environmental sustainability. This strategy acknowledges that security solutions of encryption, constant surveillance, and redundancy processing are known to raise computational demands and energy consumption. Carbon-conscious mechanisms do not accept these effects as inevitable expenditures of proper security, but instead devise a methodology that achieves security effectiveness without affecting the environment. Future directions in research are energy-efficient cryptographic algorithms that give the same security with less computation, contextual security that uses intensive protection selectively on a data sensitivity basis, and hardware-optimized implementations that use fewer extra resources on security functions [10].

Conclusion

Security-First Data Engineering Framework is a paradigm shift in the way organizations consider security and compliance in data pipelines, and makes protection a core architecture and not a peripheral one. The combination of security during the pipeline design, implementation, and operation makes SF-DEF eradicate the traditional vulnerabilities and makes the compliance management much more efficient. The framework offers both short-term operational advantages, such as increased breach prevention,

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

simplified audits, and less compliance overhead, as well as strategic ones, such as the increased trust in stakeholders and readiness to comply with regulations. Implementation issues are still present and mostly in areas concerning legacy system integration, performance optimization, and change management of the organization, but the framework offers adoption routes that are flexible enough to allow incremental implementation depending on the priorities of the organization. With regulatory sophistication on the rise, trending with threat sophistication, security-first engineering is evolving beyond the competitive advantage into a key standard that regulated industries require to balance data innovation and protection needs. The shift from reactive to proactive security is fundamentally altering how organizations view data engineering to develop resilient ecosystems that will meet the needs of emerging threats and compliance requirements.

References

[1] Joye Ahmed Shonubi, "Multi-Layered Zero Trust Architectures for Cross-Domain Data Protection in Federated Enterprise Networks and High-Risk Operational Environments," International Journal of Advanced Research Publication and Reviews, 2025. [Online]. Available: https://openreview.net/pdf?id=Pm7uC3lXf9
[2] Shivali Naik, "Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy," ESISCS, 2023. [Online]. Available: https://esj.eastasouth-institute.com/index.php/esiscs/article/view/452
[3] Mark Button and Peter Stiernstedt, "The evolution of security industry regulation in the European Union," University of West London. [Online]. Available: https://repository.uwl.ac.uk/id/eprint/6186/1/The_Evolution_of_security_industry_regulation_in_the_EU_PURE.pdf
[4] Oleksandr Kosenkov et al., "Systematic mapping study on requirements engineering for regulatory compliance of software systems," ScienceDirect, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584924002271
[5] Krti Tallam, "Security-First AI: Foundations for Robust and Trustworthy Systems," arXiv:2504.16110, 2025. [Online]. Available: https://arxiv.org/abs/2504.16110v1
[6] Adaeze Ojinika Ezeogu and Asafa Emmanuel, "Securing Big Data Pipelines in Healthcare: A Framework for Real-Time Threat Detection in Population Health Systems," Research Corridor Journal of Engineering Science, 2025. [Online]. Available: https://www.researchcorridor.org/index.php/RCJES/article/view/531
[7] Anayo Ikegwu et al., "Review of Embedded Systems and Cyber Threat Intelligence for Enhancing Data Security in Mobile Health," ResearchGate, 2025. [Online]. Available: https://www.researchgate.net/publication/393383554_Review_of_Embedded_Systems_and_Cyber_Threat_Intelligence_for_Enhancing_Data_Security_in_Mobile_Health
[8] Sai Kishore Chintakindhi, "Stream Processing Framework for Ensuring Data Integrity across High-Velocity Financial Data Pipelines," IJLRP, 2025. [Online]. Available: https://www.ijlrp.com/papers/2025/3/1574.pdf
[9] Favour Olaoye and Axel Egon, "Federated Learning for Privacy-Preserving Security Analytics," ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/383565552_Federated_Learning_for_Privacy-Preserving_Security_Analytics
[10] Yusuf Usman et al., "Green Cybersecurity: Leveraging AI, ML, and LLMs to Optimize Energy, Threat Detection, and Sustainability Frameworks," IEEE Access, 2025. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=11141387

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.